SECTION 2 - BUSINESS ISSUES

2.1 Implementation Considerations

When implementing EDI a multitude of questions must be asked and answered. How can we obtain management support? How do we justify cost? Who will be impacted by the use of EDI? These questions and a host of other questions regarding the impact of EDI on business issues will be answered in this section.

2.1.1 Establishing an EDI Committee

An EDI coordinating committee should be established. It is imperative that the EDI committee have a well defined and understood mission statement for itself and the designated project teams. This committee will be the focal point and control element for direction and communication. It should include representatives from all of the involved functions such as information systems, materials management, purchasing, sales, legal, audit, etc. The EDI committee will designate Project Teams to manage segments of the total project.

2.1.2 Implementation Suggestions

The following are implementation recommendations:

C Talk with experienced EDI users;

C Get involved with industry associations and standards organizations;

C Determine EDI objectives;

C Gain commitment from management, business units and support groups;

C Establish an EDI Implementation Team;

C Consider the extent to which internal systems are suitable for EDI;

C Select pilot partners with experience in EDI;

C Limit the initial effort to a few partners and transactions;

C Identify appropriate products with which to start;

C Begin with partnerships where transaction volumes are high;

C Integrate EDI with existing systems;

C Review tax, audit, and legal requirements;

C Evaluate hardware/software alternatives and make selections, carefully weighing the use of PC software for data entry and high transaction volumes;

C Provide an EDI training program (including training on EDI standards) for users;

C Enlist the assistance of experienced consultants and third parties;

C Establish agreements with trading partners;

C If applicable, be sure links exist to allow transmissions to flow between third parties;

C Have frequent progress discussions with partners and assign coordinator/contact;

C Define methods to handle exceptions and problems;

C Exchange documents in parallel mode for at least several cycles before initiation of live EDI data;

C Discontinue paper documents when EDI is operational;

C Publicize EDI benefits internally;

C Expand EDI efforts by establishing trading relationships with partners of varying sizes, EDI experience, and computer sophistication;

C Pursue EDI with only those partners where it makes business sense to do so;

C Participate in EDI industry and standards activities;

C Plan for significant up-front costs;

C Resist trading partners who want to use proprietary formats; and

C Get help from marketing, purchasing and other functional groups in the development of your EDI plans and architecture.

2.1.3 EDI Cost Justification

Short- and long-term benefits should be forecast when justifying the cost involved in implementing an EDI program. Trading partners face three cost categories:

C Application development costs,

C Supporting encryption when required, and

C Modifying applications to capture the reporting data required.

C Message costs.

The application development costs impact all trading partners. Trading partners existing applications will probably require some modifications. Trading partners that have no existing application will incur the development costs. There are three major cost areas:

C Modifying EDI software to access the application systems,

C Supporting encryption when required, and

C Modifying applications to capture the reporting data required.

Translation software costs vary depending on the hardware and translation software selected for use. Consult with EDI translation software providers to determine the costs.

Message costs are a function of the transactions implemented, number of transactions, volume, frequency of transmission, time of day transmitting, method of transmission (direct, VAN, dial-up, etc.), VAN costs, and other factors.

2.1.4 Strategy for Implementation

Information needs to be collected to develop a successful strategy for implementing an EDI project. Consider the following when planning your implementation strategy:

C Develop a business applications/trading partners matrix;

C Designate EDI business contacts;

C Obtain contact information for Value Added Networks (VAN);

C Obtain contact information for software providers;

C Determine what partner identification scheme should be used, (e.g., DUNS number);

- Define terms of exchange and establish an agreement between trading partners; and

- Develop an overall system data flow design.

Based on the information collected from business partners, develop an overall EDI plan. Conduct meetings/conferences with trading partners to define EDI plans and dates. Consideration should be given to those trading partners capable of doing EDI and having the desire to participate.

2.1.5 Transaction Sets

Determine the applicable ASC X12 transaction sets that will be used and the minimum data that will be necessary to satisfy the application data requirements. Determine which acknowledgements shall be used.

EPA implementations currently use, or have plans for using, the following ASC X12 Transaction Sets:

810	Invoice
820	Payment Order/Remittance Advice
824	Application Advice
841	Specifications/Technical Information
850	Purchase Order
855	Purchase Order Acknowledgment
856	Ship Notice/Manifest
860	Purchase Order Change Request - Buyer Initiated
863	Report of Test Results
864	Text Message
865	Purchase Order Change Acknowledgment/Request - Seller Initiated
867	Product Transfer and Resale
997	Functional Acknowledgment

The individual project Implementation Guidelines provide the details of the use for each transaction set.

2.1.6 Pilot Program

A pilot program is a method of initiating EDI that provides the ability to test concepts, practices, and EDI policies. A pilot program is the initial step of a production implementation schedule. The schedule should encompass the inclusion of all applicable trading partners into the EDI system. An integral part of a pilot program is to establish test criteria. These criteria must include:

- Coding and testing the interface to in-house system(s);

C Conducting system tests with translation software and network (if used);

C Conducting system tests with the trading partners using a test data file and/or testing with live data;

C Sending sample X12 data to trading partner;

C Initiating parallel processing.

2.1.7 Education

Educating internal and external personnel in EDI is vital to the success of any EDI project. User personnel should be educated as to why the company is implementing the standards and what impact it may have on the current procedures. Trading partner education regarding EDI transactions and future plans can be accomplished on an individual basis or through sponsoring trading partner conferences.

2.2 Timing of Transactions

A number of timing issues to be considered and resolved with trading partners when determining the timing of transactions include:

C When the business transaction(s) will be made available to the trading partner,

C Rules for acceptance/rejection of transmissions including time stamp of the transmission;

C Retention periods for both sender and network message storage transmission;

C Timings of the transaction acknowledgment;

C Methods of handling legal holidays;

C Deadlines for submission of the information and receipt of functional acknowledgments; and

C Abilities of the existing computer systems to respond within a specific time frame.

2.3 Modes of Operation

The two modes of operation are Production and Test. Production is used when both partners agree both systems are communicating the agreed upon data for the transaction sets implemented. The test mode is used when implementing a new transaction, when making a modification to implemented transactions, or when upgrading to a new version/release. The Trading Partners should be aware of when the test mode will be used in order to provide assistance to each other. Identification of the mode of operation is contained in the ISA (Interchange Control Header) Position ISA15, Data Element I14. A "P" identifies production data and "T" identifies test data.

Trading Partner systems must have the provision to handle both production and test transaction sets.

2.4 Security

The risks inherent in the EDI process are based on the lack of paper documentation to backup the transactions. EDI involves the transmission of electronic messages, or records, that may never be converted to hard copy. Therefore, the electronic records must be able to stand alone as submission data. These records are subject to the same security requirements as are all types of EPA data.

The EDI process must include all steps necessary to ensure that the records are authentic, are properly authorized, and are retained in a manner that will ensure the integrity of the records. Audit trails must be maintained for accountability.

The *integrity* of EDI messages is essential. Security controls must be in place to ensure that the message is not modified and that electronic records are protected from loss or destruction. In addition, if EDI messages contain sensitive or Confidential Business Information (CBI), adequate controls must be in place to protect the data from inappropriate disclosure.

The *authentication of the originator* is a critical security issue for EDI. The process must be able to ensure that the source of the message is the named originator.

Computer security plans must be developed for EDI. The resources allocated to protecting EDI systems must be based on the risk and magnitude of potential harm that could result from the loss, misuse, or inappropriate access to or modification of EDI data. Specific controls should be implemented for the following aspects of the EDI system:

Integrity - Controls, such as audit trails, access control mechanisms, and separation of duties must be in place to protect the integrity of EDI data. Controls within the EDI environment for protecting data integrity include the following techniques:

C Recalculating and verifying real totals and hash totals for critical parameters

C Repeating messages or parts of messages rather than using only a functional acknowledgement.

C Including unique identifier codes within each message to define each message as a separate distinct message.

Confidentiality - EDI systems processing confidential data, such as Privacy Act, CBI, or enforcement data must include access controls to restrict access to authorized personnel only. Access controls include technical controls, such as passwords or encryption, as well as procedural controls, such as restricted access to physical areas processing confidential data.

Availability - Contingency plans must be prepared to provide for continuity of operations in case of system failure or system degradation. Contingency plans should include backups on a periodic basis commensurate with the importance of the data maintained within the system. The contingency plan must also be tested periodically to ensure that it accounts for all possible threats to system and data availability.

Authentication - Authentication controls must be in place to ensure that the source of the message is the named originator. Non-repudiation should be used when authentication is a critical issue. Specific techniques for authentication include:

C Returning an acknowledgement for each message sent. A valid message will send an acknowledgement to the originator within a pre-specified time period

C Utilizing specific log-on techniques.

C Including secret (known only to the parties involved) reference numbers or passwords within the body of the message.

Written agreements - Written agreements can be used to stipulate the specific security and authentication mechanisms to be used.

In addition, cryptographic techniques should be considered, especially for high-risk systems, to protect the confidentiality, integrity, and authentication of EDI systems.

Procedural controls can be implemented to protect the integrity, availability and confidentiality of EPA's information and systems. Procedural controls may be less expensive and easier to implement than technical controls. Procedural controls can include activities such as limiting physical access to data entry or computer areas, providing security training, creating security procedure manuals, and requiring separation of duties.

The laws and regulations mandating safeguards mandating safeguards for Federal information and information systems include:

- The Privacy Act of 1974 (P.L. 93-579);
- The Freedom of Information Act (5 U.S.C. 552);
- The Paperwork Reduction Act of 1980 (P.L. 96-511);
- The Computer Security Act of 1987 (P.L. 100-235); and
- U.S. Code, Title 18, Section 1905

.

The organization that initiates an EDI system should take care to avoid making unreasonable demands of its trading partners. While the initiating trading partner may have the Resources and expertise to handle an EDI system easily, this may not always be true of the other partner(s).These limitations of resources and expertise should be taken into account. Please refer to the individual project EDI Implementation Guideline for specific security requirements.

2.5 Backup and Recovery Procedures

Backup and recovery procedures are necessary to provide:

- Retransmission capabilities;
- Translator re-run capabilities;
- Minimum 24- to 48-hour immediate access backup; and
- Archive and recovery capabilities for individual EDI transactions.

The backup and recovery procedures must be thoroughly documented to allow anyone with the proper authority to access the system to retransmit data.

It will be up to each EDI partner to keep their own records and archives of EDI transactions sent and received. Either partner must have the capability to retransmit an EDI message.

The Functional Acknowledgement (997) transaction set can be used to provide a level of automation in the backup and recovery area. If the EDI system expects to receive a Functional Acknowledgment for every transaction it sends, the EDI message should be available for retransmissions until a Functional Acknowledgement corresponding to a specific EDI message is received. Once the Functional Acknowledgment is received, the original EDI message can be archived regardless of the normal archive timing.

The Agency requires the use of the Functional Acknowledgment. The Functional Acknowledgment is used to confirm receipt of the Trading Partner's transmission and indicate acceptance or rejection of the transaction set by the translator. A Functional Acknowledgment is not required for a transmission of Functional Acknowledgments.

2.5.1 Disaster Recovery Considerations

Disaster recovery becomes correspondingly critical to the amount of business that is conducted through the EDI channels. Consider the consequences to you and your trading partners if you were suddenly unable to exchange transmissions for an extended period. It is unwise to assume that you can fall back on a paper-based system. Your trading partners may not be able to quickly switch from EDI messages to mailing their business transactions to you. You may not have immediate access to the resources within your organization needed to process paper transactions.

Develop a plan to deal with extreme problems, such as a total loss of a Data Center or computer system and a loss of a phone company switch station servicing your area.

2.6 Audit Considerations

One of the first questions raised when considering the use of EDI relates to its impact on controls. Without a signed document and a paper audit trail, how will one know when a transaction is valid and approved?

The same elements of control will exist in an EDI-based system that exist with a paper-based system. Most controls related to EDI fall into three categories: confidentiality, integrity, and authenticity. Confidentiality is the control that allows only authorized persons access to the transactions. Integrity controls validation of the data. Authenticity is the control that ensures the receiver that the transaction received is valid and belongs to them.

The following are specific examples of controls within the confidentiality, integrity, and authenticity control categories.

Confidentiality

C Encryption is a method of logically scrambling the EDI information with an encryption key and giving the key only to persons who have a right to that information. The key is an electronic code for this procedure.

C Password protection is a method used to control access to files. Passwords should be changed often for maximum effect.

C The use of a stand-alone computer for receiving EDI transmissions controls access to the main computer. Once the EDI data is on the stand-alone computer, it can be validated and uploaded to the main computer for use in applications.

Integrity

C Communications protocols provide bit count checking.

C Every X12 transmission contains Segment, Transaction Set, and Functional Group counts. Hash Total and selective segment counts are provided by certain transactions. Functional Acknowledgments are available to confirm transaction receipt and compliance to the standard.

C Translators provide code validation and syntax checking.

Authenticity

C Value Added Networks (VANS) validate:

- Sender/receiver identifications
- Passwords

C Translator Trading Partner Profiles validate:

- Sender identification
- Password
- Version/Release
- Transmission sequence
- Transaction Set

C Application programs validate:

- Personal Identification Numbers (PIN)
- Specified data contained in the Transaction Set (i.e., dates, reference numbers).